Monitoring ISDN links

[30980016 WO]

Technical Field

This invention relates to monitoring systems which collect data from an Integrated Services Digital Network (ISDN).

Background

The Integrated Services Digital Network has been designed to provide customers with digital access to the public network, which can carry a number of different services at a range of different bandwidths. The narrowband ISDN is extensively deployed worldwide. The broadband ISDN (B-ISDN) is in early deployment and trial phases with a number of operators. The network that operators will actually have to manage will be a combination of existing digital and analogue networks, narrowband ISDN, broadband ISDN, internet technology and other technologies. A specific service is likely to use resources from a number of these different networks (Figure 2 shows some examples of the resources and technologies involved). This presents major problems in the end-to-end management of the service. The monitoring system described here addresses many of these problems.

Disclosure of Invention

According to one aspect of this invention there is provided a method of monitoring an ISDN link, comprising the steps of: monitoring at a first location subscriber signalling messages on an ISDN D channel to derive first monitoring data; monitoring at said first location telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and correlating said first and second monitoring data.

In some case it may be desirable to monitor additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network (such as the public switched telephone network – PSTN) coupled to said ISDN link, to derive third monitoring data, and correlate those third monitoring data with at least one of the first and second monitoring data. Another option is to monitor signalling messages and telecommunications traffic on ISDN links at a second location, and correlate the resulting monitoring data with those first and second monitoring data.

According to another aspect of this invention there is provided a method of monitoring an ISDN link, comprising the steps of: monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and correlating said first and second monitoring data.

According to a further aspect of this invention there is provided apparatus for monitoring an ISDN link, comprising: first equipment at a first location for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; second equipment at said first location for monitoring telecommunications traffic traversing ISDN B channels associated with said ISDN D channel to derive second monitoring data; and correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

According to another aspect of this invention there is provided apparatus for monitoring an ISDN link, comprising the steps of: first equipment for monitoring subscriber signalling messages on an ISDN D channel to derive first monitoring data; second equipment for monitoring additional signalling messages (e.g. SS7 protocol messages) on a signalling link in a telecommunications network coupled to said ISDN link, to derive second monitoring data; and correlation apparatus coupled to said first and second equipment to receive and correlate said first and second monitoring data.

Brief Description of Drawings

Methods and apparatus in accordance with this invention for monitoring ISDN links will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 shows a distributed ISDN monitoring system;

Figure 2 shows examples of local loop and core network probe measurements which may be correlated to create end-to-end service records; and

Figure 3 shows one exemplary architecture for combined monitoring of an ISDN and an SS7 signalling system.

Best Mode for Carrying Out the Invention, & Industrial Applicability

The distributed monitoring system shown in the drawings has the capability to collect data from an ISDN, correlate these data in real-time, and provide a real-time view of services on the network. These data can be used for applications such as troubleshooting, surveillance, security, network planning, provision of accounting information to customers, fraud detection, billing and marketing information. The monitoring system can be used to monitor multiple ISDNs which may be interconnected by other technologies, such as internet protocol (IP) networks. Part of the ISDNs may be made up of older technologies, such as analogue.

Referring to Figure 1, the probes shown are part of a distributed monitoring system, and may be implemented as either link monitoring devices (using techniques similar to those in existing protocol analysers for example) or as software and hardware on network elements (such as nodes and switches). The distributed monitoring system is

constructed from the probes and standard computer and communications components, with specialised software which provides the applications described above. A principal function of this specialised software is to correlate data from different probes to provide a record or real-time trace of calls, transactions and other services as they occur on the network. The Hewlett-Packard *acceSS7* system is an example of a distributed monitoring system which could be used to implement parts of the system described above.

According to this invention monitoring of the local loop is also provided, in respect of subscriber signalling and the services themselves (for example the content of the B channels of primary rate access (PRA) or basic rate access (BRA) ISDN); furthermore data from any of the probes covering any of the technologies in the local loop or core network (see Figure 2) may be correlated (e.g. data from a probe for any local loop protocol at one end of the service, plus data from a probe for any core network protocol, plus data from a probe for any local loop protocol at the other end of the service).

An example of a monitoring system architecture is given in Figure 3. This shows probes passively monitoring both the SS7 network and the PRA ISDN. The SS7 passive-monitoring probes could be for example from the Hewlett-Packard *acceSS7* system. The ISDN primary rate access probes could for example be constructed using the same techniques as in existing protocol analysers (such as the Hewlett-Packard 37900D Signalling Test Set).

According to this invention the distributed monitoring system is arranged to correlate real-time data from any combination of these probes. This includes, for example, the D channel and B channel of ISDN PRA and the signalling units from SS7.

The invention can be applied in respect of other protocols and technologies in the access network. An important example is the use of remote digital terminals to concentrate a number of different local loop technologies to a common interface. The local loop technologies supported are: traditional analogue connections, ISDN primary rate and basic rate, various copper-pair based high-speed digital subscriber loop technologies (e.g. ADSL, HDSL), "Fibre in the Loop" and wireless technologies. The ITU-T V5 specification and the Bellcore GR-303 series of specifications are examples of architectures used to concentrate the subscriber loop technologies. Probes can be constructed which monitor the connection between the digital terminal and the local switch (e.g. the V5 or GR-303 protocol), using technologies already available for protocol analyser products such as the HP 37900D. The probes can determine the signalling protocol on the connection, and monitor the bearer channels, in a similar way to the ISDN monitoring architecture shown in Figure 3. This data source should be considered part of the distributed monitoring system for the following discussion. Service usage data can be obtained from this source in a similar way as for ISDN, but for a broader range of subscriber loop technologies.

For convenience the invention is described primarily with reference to narrowband ISDN and its associated B (bearer) channels and D (data) channel. However, it should be understood that this terminology is to be taken as including within its scope channels with analogous functionality in broadband ISDN systems, such as asynchronous transfer mode (ATM) systems, whether or not they are customarily identified by these terms.

The analogue of the D channel in the broadband ISDN is a predefined virtual channel called the Signalling Channel. In the case of non-associated mode signalling this channel is identified by Virtual Path Identifier (VPI) = 0 and Virtual Channel Identifier (VCI) = 5. In the case of associated mode signalling there is an independent signalling channel for each virtual path that is using associated signalling. This signalling channel has the same VPI as the virtual path and VCI = 5.

The analogue of the B channel in the broadband ISDN is a dynamically assigned virtual channel (sometimes called a Switched Virtual Circuit or SVC), which is set up using messages on the signalling channel, and which carries the communication traffic between the two communicating endpoints. This can be identified by capturing and decoding of the relevant signalling messages on the signalling channel, as described in more detail later.

GENERATION OF SERVICE RECORDS

This section lists the types of fields in various examples of service records, and describes how the distributed monitoring system could provide the required data. A service record is generated for each instance of the usage of a specific service. This is a generalisation of a call record, which is generated by current switches. A service is normally defined from the perspective of the user. The service may actually involve a number of calls or transactions, for example. The service records described here correlate together these different calls and transactions, using information from the SS7 and ISDN signalling information, to provide a single record of the service.

1. Calling Party Information.

This includes any information which can be derived about the calling party from the data flowing on the links of the Integrated Services Digital Network, and is therefore available to the link monitoring probes. Typical information includes: calling party number; any ISDN sub-addressing information; calling party name; X.25 or frame relay addresses; other network addresses; and any numbers or addresses related to billing.

This information may be derived from: call setup messages on the ISDN D channels, at either the originating or terminating end or both; and/or from call setup messages on any of the SS7 links. Additional information may be derived from the ISDN B channel for certain services such as frame relay. In this case the headers of the frames

contain addressing information. Additional information may also be derived from any intelligent network services messages which flow over the SS7 links as part of the specific service usage. Further information may be derived from looking at the ISDN B or D channels of any intelligent peripherals involved in the specific service usage.

2. Called Party Information.

As for calling party information, but replace calling party by called party.

3. Network Routing Information.

This may include any information on the network resources which were used to provide this specific service usage. The following are examples of data which might be provided:

- ISDN links and channels used;
- SS7 links and nodes used;
- trunks used;
- intelligent network nodes used.

Each of these uses is time-stamped, and the sequence and nature of the use indicated.

These data can be obtained in a similar way as was described for item 1 above.

4. Intelligent Network Services Information.

This may include any information on intelligent network services used for this specific service usage. The following are some examples of the data which may be provided:

- calling party name delivery information;
- local number portability information;
- call forwarding information;
- interactive voice response information on the use of intelligent peripherals;
- 800 number services.

This information includes time-stamps, duration and the nature of the use.

These data can be obtained in a similar way as was described for item 1 above.

5. Service Status and Termination Information.

This may include time-stamped information on the initiation of the service, any status changes occurring during service and the termination of the service. The termination information should include the reasons for termination.

These data can be obtained in a similar way as was described for item 1 above. In particular, the call clearing messages on the SS7 links and the ISDN D channels can provide details on the reasons for call termination.

6. Analysis of B-Channel to Distinguish Voice from Fax or Data.

As part of the process of generating service records, the B-channel associated with a particular call can be identified from the signalling messages on the corresponding D-channel. The probe monitoring the link carrying the B-channel can be instructed to capture data from the B-channel. An analysis of the spectrum of this captured data can be used to identify the type of service being carried in the B-channel. This could be used for distinguishing a voice call from a fax or data call. The probe can be instructed to periodically sample the B-channel to check for any change in the type of service being used.

7. Analysis of Tones in the B-Channel to Identify Any Additional Dialled Data.

The probe may also be instructed to analyse the data captured from the B-channel to identify any multi-frequency tones (eg DTMF) which may provide further information about the call. This may be used to identify any additional digits dialled by the subscriber after the initial call is connected. These digits can be added to any service record which is generated by the monitoring system for the call. It could also used for identifying a fax call from the signalling between two fax machines.

8. Service Type.

This may include information on the following types of services:

- voice;
- modem;
- fax;
- video;
- X.25;
- frame relay;
- ATM (asynchronous transfer mode);
- LAN interconnection.

These data can be obtained in a similar way as was described for item 1 above. In particular, the call establishment messages in the ISDN D channel provide information on the type of service. This can be correlated with data taken from the ISDN B channels identified in the ISDN D channel signalling.

9. Service Quality Information.

The service quality information provided is dependent on the service indicated in the service type field. The following gives some examples of what can be provided for specific services.

Voice quality is mainly indicated by the bit error rate and the delay. These parameters can be measured using a passive monitoring system, by using the signalling

information to identify the ISDN B channels which are carrying the voice signals. The bit streams from each of the B channels identified can be compared to derive the delay and bit error rate caused by the intermediate networks. This is particularly important where one of the intermediate networks is packet or frame based and cannot guarantee delivery times (e.g. IP protocol or ATM).

Video, modem and fax quality can be addressed in a similar way.

The data oriented protocols (X.25, frame relay, ATM and LAN interconnection) require additional data. These can again be measured by using SS7 or ISDN signalling data from the probes to identify the ISDN channels carrying the protocol. Existing protocol analysis techniques can be used to provide estimates of parameters like packet loss, retransmissions, CRC errors, throughput and packet delay.

10. Service Usage Information.

The time of usage data provided by the distributed monitoring system depends on the specific service. Some examples follow.

Voice, video and fax services require call duration and allocated bandwidth.

The data oriented services require data such as total bits, frames and packets in each direction. This may be provided for regular time intervals for the duration of the service. It may also be broken down into a traffic matrix, where the data protocol has additional addressing information (such as IP addresses). The data are obtained in a similar way as is described for item 9 above.

11. Security Information.

A particular instance of service usage may be an attempt to obtain unauthorised access to resources. The service record includes information which may indicate this type of behaviour. This may include information about the duration of call, the way the call was terminated and details of the service used.

An example would be where a modem is used repeatedly to try different passwords. The ISDN B channel used is identified from SS7 and ISDN signalling data. The probes then extract the data from the ISDN B channel, and the system can determine the modem protocol to identify behaviour.

The examples described above focus mainly on narrow band ISDN. However the same concepts apply to broadband ISDN and ATM. Variants of the Q.931 protocol are used in these standards for users to network interface signalling (UNI) and network to network interface signalling (NNI). These can be monitored in a similar fashion, and service records generated from the sequence of messages which control a particular call. The concept of channels is replaced by the concepts of virtual paths and virtual channels. However, the virtual path and virtual channel associated with a particular call can be

identified from the signalling messages, and the probes monitoring the links which carry these virtual paths and channels can be instructed to capture the data associated with the call and provides an analysis similar to the narrow band case for inclusion in the service record which is generated.

REAL-TIME UPDATES ON SERVICE USE

The data that populates the service records described in the previous section is collected in real-time from the monitoring probes. These data can be provided in real-time on remotely connected computers as they becomes available. A user of the distributed monitoring system can apply filtering criteria on any of the information described in the previous section, to select those instances of service use for which real-time updates are required.

APPLICATIONS

The following applications can be implemented using the data from the service records described above or the real-time service updates. Data from other sources may be used to enhance the effectiveness of these applications.

A. Quality of Service and Service Level Agreements.

The service records described above can be used to provide service quality information on selected customer's service. This can be used to track conformance to service level agreements, and be provided to the customer as an additional service. It can be provided as periodic reports, or in real-time using the real-time updates described above.

B. Surveillance and Troubleshooting for Network Operations.

The service records and real-time updates can be used to identify service or network faults. The information can also be used to troubleshoot the faults.

C. Fraud Detection.

The service records and real-time updates can be used to identify potential fraudulent use of the network or service. Indications may include excessive use of high value services, unusual call termination behaviour and repeated failures to gain access to a service. The distributed monitoring system may be used to track the service usage of potential high-risk users in real-time.

D. Security and Hacking Detection

Potential security threats can be identified by repeated failures to gain access to a service. They also may be indicated by successful access to sensitive services, such as

maintenance ports on customer premises equipment (CPE). This type of data is available from the service records and the real-time updates.

E. Billing Data

The service records can be used as a basis for billing which is dependent on any of the fields in the service record. This allows, for example, billing to be based on the actual service quality delivered. It also enables billing to reflect the nature and generation of the usage of resources on the network, such as intelligent peripherals and databases.

F. Use of B-Channel Data for Billing or Billing Verification Purposes.

In some countries the regulatory requirements for Telecom operators require that calls carrying voice have a different tariff to calls carrying data. They also require that any access charges between operators depend on whether the call is voice or data, and if it is voice there is also a dependency on the final destination for call. The service records generated by the monitoring system can be used to determine the bill in these cases (and similar situations), using the data derived from the B-channel as described in respect of items 6 and 7 above.

G. Customer Accounting Data

The detailed service usage information in the service records can be provided to customers for use in their internal accounting. This includes the traffic matrix information for packet and frame based protocols, which the system derives from the B and D ISDN channels.

H. Customer and Telecom Operator Network Planning

The service records can provide detailed information on the use of network resources which can be provided to network planning departments within the operator and the customer.

SS7 SIGNALLING NETWORKS AND VOICE TRUNK NETWORKS

1. A Monitoring System to Provide Call Records Containing Data from Both the SS7 Signalling Network and the Trunk Network.

A monitoring system such as Hewlett-Packard's *acceSS7* system can be used to generate call (or service) records by monitoring the sequences of messages on the SS7 network. This monitoring system can be extended with probes which monitor the trunks which carry the voice path for calls. The trunk carrying the voice path for a particular call can be identified from fields with in the SS7 messages (normally the TCIC in the IAM). The probe connected to this trunk can then be instructed to capture the data from the trunk for analysis in real-time or at a later date.

2. Analysis of "Voice Path" to Distinguish Voice from Fax or Data.

As part of the process of generating service records, the trunk associated with a particular call can be identified from the signalling messages on the corresponding SS7 network. The probe monitoring the trunk can be instructed to capture data from the trunk. An analysis of the spectrum of this captured data can be used to identify the type of service being carried in the call. This could be used for distinguishing a voice call from a fax or data call. The probe can be instructed to periodically sample the trunk to check for any change in the type of service being used.

3. Analysis of Tones in the "Voice Path" to Identify Any Additional Dialled Data.

The probe may also be instructed to analyse the data captured from the trunk to identify any multi-frequency tones (eg DTMF) which may provide further information about the call. This may be used to identify any additional digits dialled by the subscriber after the initial call is connected. These digits can be added to any service record which is generated by the monitoring system for the call. It could also used for identifying a fax call from the signalling between two fax machines.

4. Use of "Voice Path" Data for Billing Purposes.

In some countries the regulatory requirements for Telecom operators require that calls carrying voice have a different tariff to calls carrying data. They also require that any access charges between operators depend on whether the call is voice or data, and if it is voice there is also a dependency on the final destination for call. The service records generated by the monitoring system can be used to determine the bill in these cases (and similar situations), using the data derived from the "Voice Path" as described above.

EXAMPLE OF IMPLEMENTATION FOR B-ISDN USING ATM

A more detailed description of an implementation for a broadband ISDN using ATM will now be given.

ATM infrastructure including UNI and NNI signalling, and potential monitor points: the probes monitor ATM links which may support a User Network Interface (UNI) of a Network Network Interface (NNI). These may be public, private or inter-carrier interfaces - section 4.1 of the ITU-T standard Q.2931 "B-ISDN Application Protocols For Access Signaling" gives more details of these interfaces.

The probes monitor one or more of the links in the ATM network and have the capability to correlate data between them, as indicated in Figure 1.

Description of ATM probe including passive optical tap: the ATM probes monitor the links by means of an optical power splitter which has been physically inserted into the

optical link. This ensures that the probe cannot modify the transmissions on the link. The probe takes a percentage of the optical power (typically 10%) and uses this to provide a copy of the ATM cells which are being carried by the link. The probe has hardware (e.g. processor, memory and input/output interfaces) and software enabling it to decode the ATM protocol and the higher level protocols being carried over the ATM layer.

The Generation of Service Records (SRs) for Switched Virtual Circuits (SVCs, also referred to as calls):

Step 1. Configuring the Service Record Collection System.

Collection criteria are specified for the monitoring system. This may be performed by a system administrator, or programmatically by a software application. The criteria may include a list of probes which should be instructed to monitor for signalling SETUP messages (see section 6.3.1.6 of "Private Network - Network Interface Specification" Version 1.0 (PNNI 1.0), ATM Forum af-pnni-0055.000, March 1996) which match a set of filtering criteria. The filtering criteria identify characteristics of the fields in the SETUP message. These will typically require matching to all or part of the Calling or Called Party Number Information Element (see section 4.5.11/13 of Q.2931 referenced above) of the SETUP message. An E.164 address is the most likely address type, but other types of addresses, (e.g. Network Service Access Point (NSAP) or private numbering plans) could also be supported.

A second part of the collection criteria may specify which measurements should be made on calls which match the filtering criteria.

A third part of the collection criteria may specify which measurements or call information should appear in the Service Record generated for that call.

A fourth part of the collection criteria may specify that a partially complete Service Record is sent in real-time at a specific point in the call.

Step 2. Capture each SETUP message on the Signalling Channel and match against filtering criteria.

Probes which have been instructed to monitor for setup messages will capture all setup messages from the Signalling Channel (as explained above, this is identified by VPI = 0 and VCI = 5 for non-associated signalling, or VCI = 5 and all VPI for associated signalling) and keep those that match the filtering criteria. A time stamp is also generated at the time of capture and stored with the SETUP message.

Step 3. For each setup message which matches the filtering criteria, create a Service Record (SR) and populate with information from the SETUP message.

Any of the information elements in the SETUP message can be decoded and analysed and the information used to populate the SR. The time stamp associated with the SETUP message is also stored in the SR.

Step 4. Identify the Virtual Circuit Associated with the Call.

The SETUP Message or subsequent signalling messages which are part of the same call may carry information which identifies the virtual circuit which will carry the communications associated with the call. Typically the Connection identifier information element call for the SETUP message will identify the VPCI/VCI for the virtual circuit. However, this information may be carried in a subsequent CALL PROCEEDING message. In this case the Call Reference information element (section 4.3 of Q.2931) from the SETUP message is extracted, and the probe is instructed to capture any CALL PROCEEDING message (section 6.3.1.2 of PNNI 1.0) which has the same Call Reference value. Care is needed to distinguish between calls in opposite directions, which may use the same Call Reference - the 'call reference flag' is used to do that. The VPCI/VCI for the virtual circuit can then be identified from the CALL PROCEEDING message.

Step 5. Identify the Virtual Circuit Associated with the Call At Other Monitoring Points.

Any probe on a link which carries a given SVC will capture the SETUP message and start to generate a service record for that SVC. This problem with duplicate service records can be avoided by configuring the monitoring system (in step 1) to only capture SETUP messages at ingress links (or only at egress links). However, certain measurements are made possible if two measurements points are available; this is particularly useful where the ingress and egress points are monitored.

The SETUP messages corresponding to the same SVC will have the same Calling and Called Party Number information elements. This information is sent to a common correlation point from where the probes can be instructed to make two point measurements in real-time. Alternatively the Calling and Called Party Number Information in the service records can be used at a later point to combine service records for the same call into a single record. Two point measurements such as cell loss can be computed as part of this process.

Step 6. Perform Quality of Service Measurements On the Virtual Circuit.

Single point measurements -- an example of a single point measurement which can be performed once the virtual circuit carrying the communication has been identified, is throughput analysis. The number of bytes or cells transmitted is measured at a number

of time intervals during the call. The distribution of throughput (in bytes per second for example) can be computed. A broad distribution indicates significant fluctuations in throughput. This would cause problems for any application which requires constant throughput.

Other examples of single point measurements are computation of the call setup time and the measurement of the application response time for higher level protocols such as TCP/IP.

Two point measurements -- a simple example of a two point measurement is to count the number of cells transmitted on the virtual circuit at the two monitoring points. The difference between the two numbers will give the cell loss. This measurement can be made for the call as a whole, or at time intervals during the call.

Other examples of two point measurements are measurements of the delay variation between cells, between the two measurements points.

These quality of service measurements can be included in the service record for the call, or used to produce overall statistics for the quality of service provided by the network.

Step 7. Perform Usage Measurements On the Virtual Circuit.

Usage measurements are computed at a single point. Simple examples are the counts of the bytes, cells or protocol data units. These may be stored as part of the service record for the call. More complex measurements, such as traffic matrices for the higher level protocols, may be stored as separate records associated with the call. An important example is the generation of IP flow records for calls which carry IP traffic. This may be used to provide a real-time stream of IP flow records to other applications.

Step 8. Monitor the signalling virtual channel continuously for RELEASE messages corresponding to the SETUP messages which match the filtering criteria. The RELEASE and SETUP messages are matched using the call reference value, and used to trigger the following steps: populate the service detail record with the termination time and any fields relating to the reasons for termination; instruct the probe to stop monitoring for the RELEASE message; and mark the service detail record as complete, and optionally forward to applications servers or storage servers.

A time-out should also be provided to terminate monitoring for the RELEASE message, and mark the service record as complete, if a RELEASE message is not found within the time-out period.